Model-Based Development (MBD) Coming soon to a theater near you

Resolving MBD against DO-178B

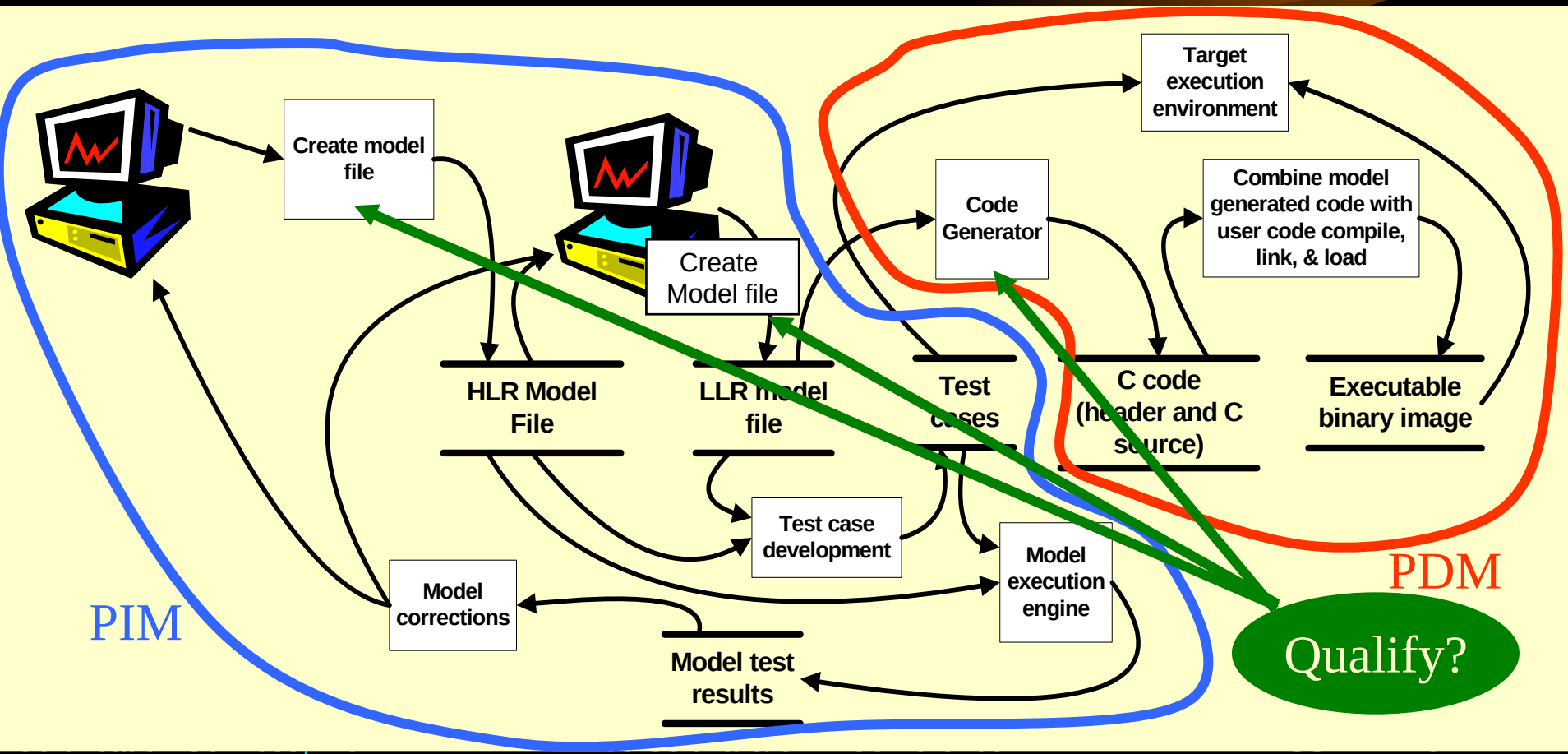
Mike DeWalt
Chief Scientist, Aviation Systems
Certification Services, Inc.
+1.360.376.8110 voice
Mike.DeWalt@certification.com

Goals

- Graphical vs. textual debate
- High- and low-level requirements, tool use
- Tool qualification
- Tool credit and DO-178B
- The great execution debate
- Examples

A tool for all seasons

- MBD with and without tool qualification



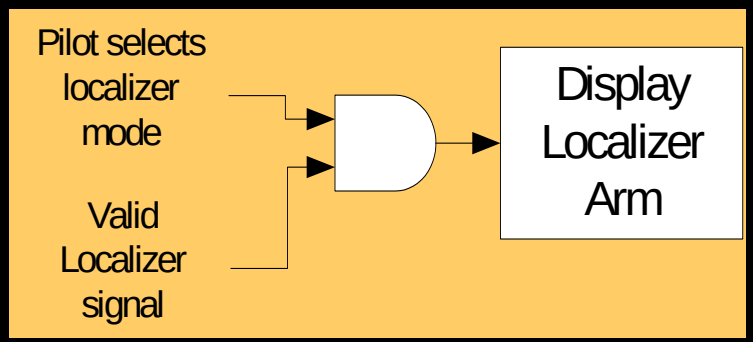
Graphical vs. textual debate

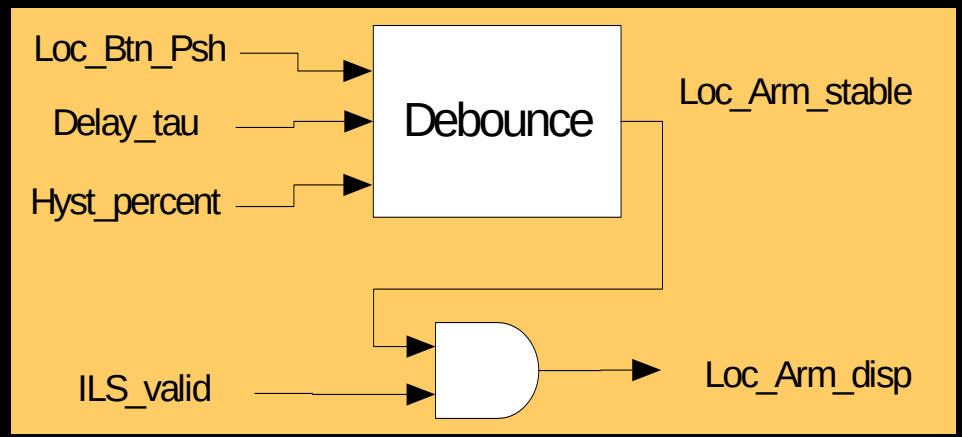
DO-178B definitions of high- and low-level requirements

- High-level requirements - Software requirements ***developed from*** analysis of ***system*** requirements, ***safety***-related ***requirements***, and system ***architecture***.
- Low-level requirements - Software requirements ***derived from high-level*** requirements, ***derived*** requirements, and design constraints ***from which source code can be directly implemented without further information***.
- Assumes continuous refinement process with constraints on lower abstraction levels – examples a/c→Sys→SW…

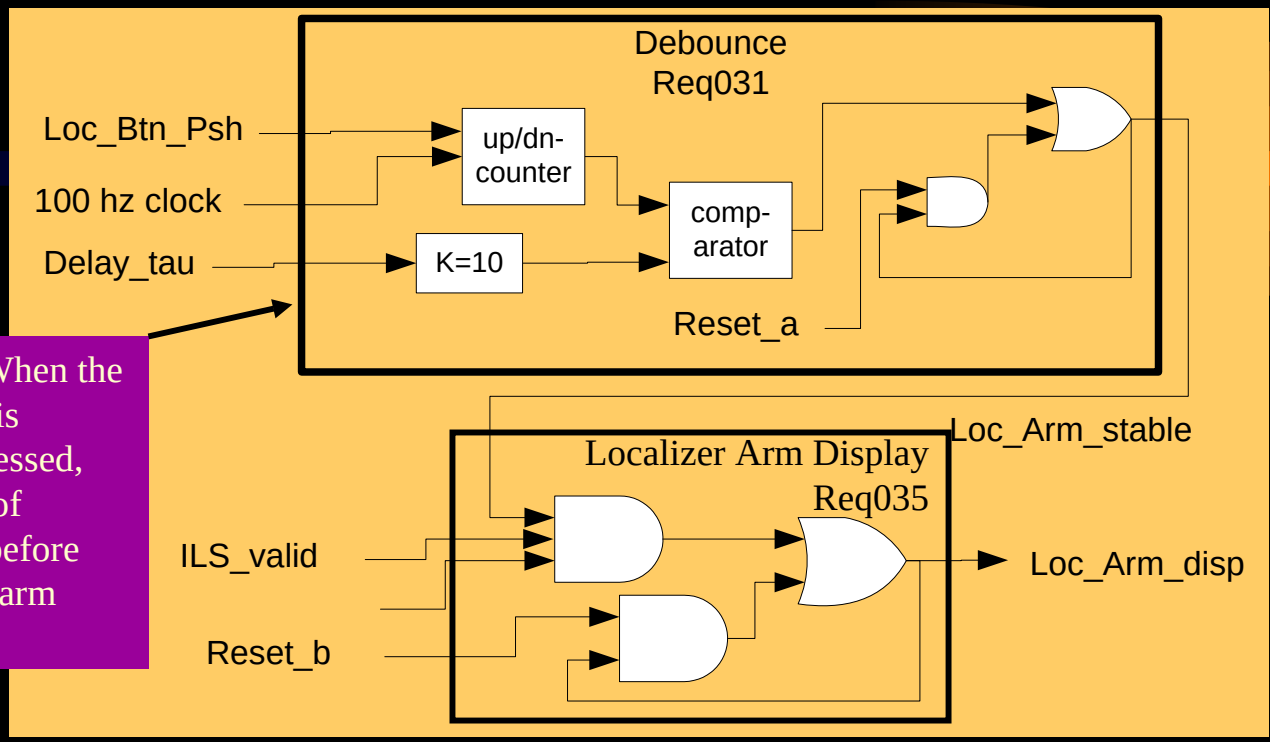
Equivalent high-level requirements representations

- A. The airplane shall display the localizer-arm indication when the pilot has selected the localizer mode and there is a valid localizer signal.
- B. The autopilot shall display the localizer-arm mode when the autopilot detects localizer mode button has been depressed and the localizer flag is valid.
- C. The autopilot shall display LocArm mode when (LocModeSel = True) .AND. (LocModeSel=stable).AND. (LocRecvr = True) .
- D.

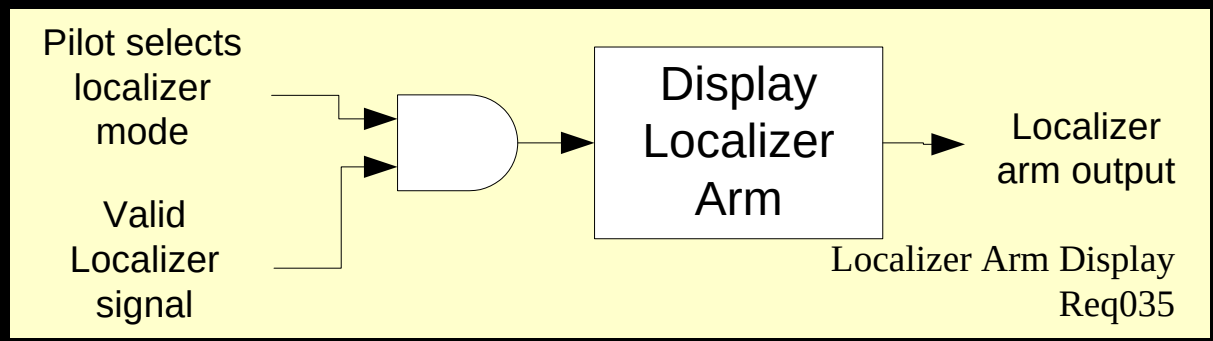




Problem: abstraction gap

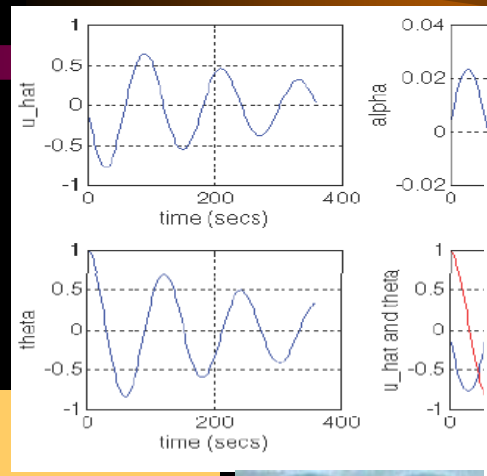


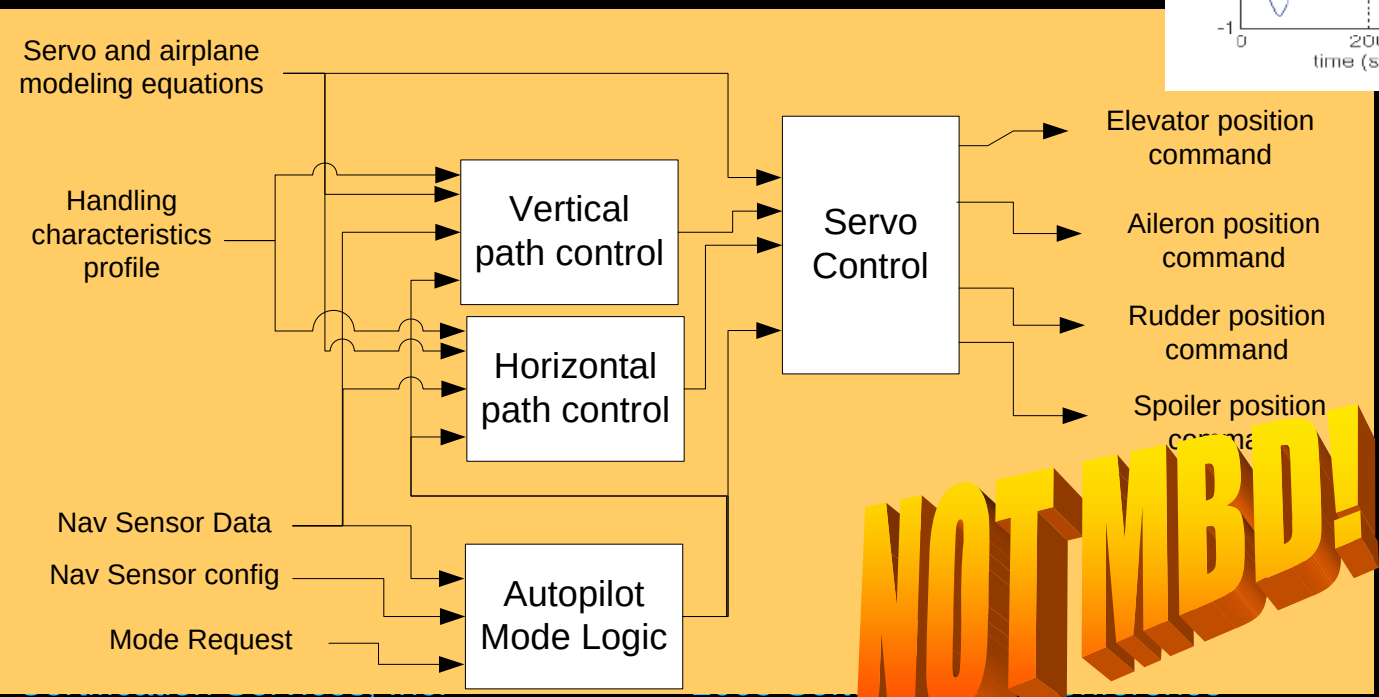
Note Req031: When the localizer button is detected as depressed, wait .1 seconds of constant signal before setting localizer arm display to arm.



Indisputable high-level requirements development tools

- VAPS
- mdAutoLand





MBD tool credit and DO-178B

- 178B – refinement model (rewriting errors)
- Abstraction gaps and qualification approach
  - (HLR to LLR) vs (.src to .obj)
  - HLR to .obj
- Out-of-the-box vs whole-table approach vs objective-by-objective approach
- MBD composed of a set of tools – boils down to tool qualification

Tool credit

- Goal of objectives: to reduce in-service errors by operating on error classes
- Approach using Annex A
  - What objectives are being made obsolete?
  - How are associated errors mitigated?
- Approach using alternate means (safety case)
  - How is correct behavior assured?
  - How are emergent errors mitigated?
  - What is the role of properties?

Criteria for Annex A objectives

- Objective satisfied by tool – partially/fully
- Objective requires manual conventional effort – partially/fully
- Assumptions needed for satisfaction
  - User (restricted constructs, use of tool, etc.)
  - Development environment (host, compilers, options, etc.)
  - Target environment (i386, PPC, I/O, etc.)
  - Execution environment (RTOS, scheduling, data formats, additional procedures, etc.)

Compliance data

- Credit analysis document (178B section 11.32)
- Organize by table or by objective
- Similar to AC 20-148 (RSC)
  - Credit (full/partial)
  - Assumptions
  - Additional activities and associated evidence

Example form

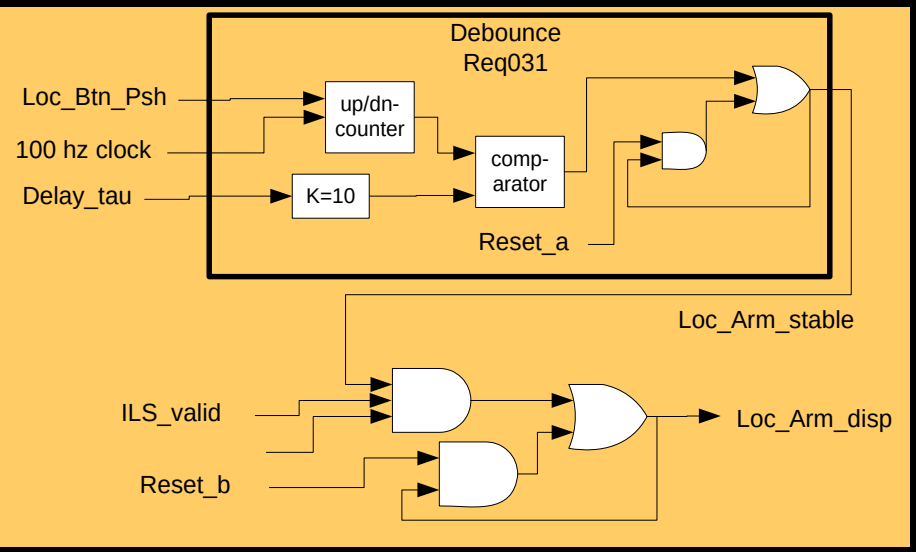
- Free template: cathy.vierthaler@certification.com

	Verification of outputs of software coding and integration processes	Credit assessment	Assump-tions	Additional user activities	Credit justification
5-1	Source code complies with low-level requirements. 6.3.4a				
5-2	Source code complies with software architecture. 6.3.4b				
5-3	Source code is verifiable. 6.3.4c				
5-4	Source code conforms to standards. 6.3.4d				
5-5	Source code is traceable to low-level requirements. 6.3.4e				
5-6	Source code is accurate and consistent. 6.3.4f				
5-7	Output of software integration process is complete and correct. 6.3.5				

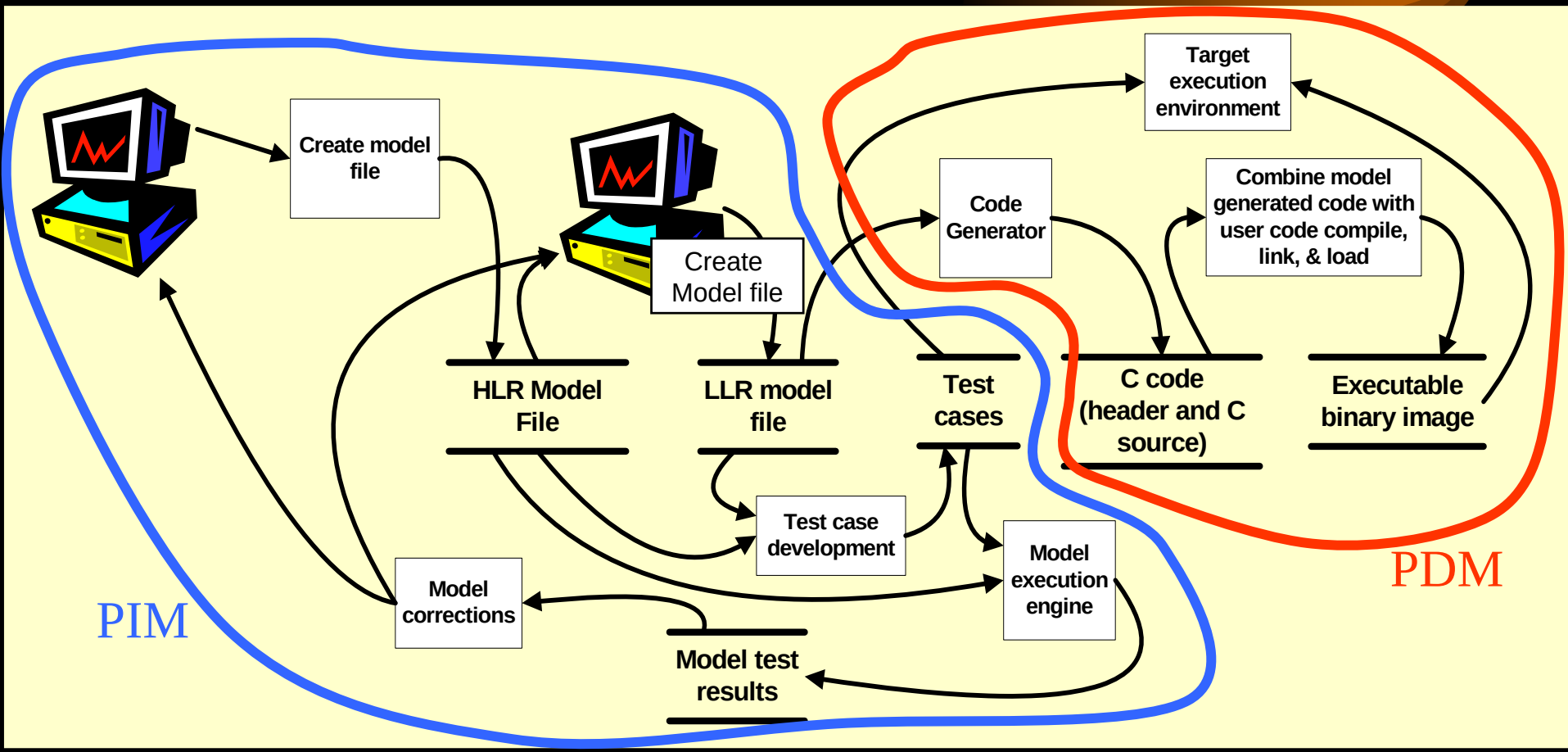
Example: Annex A, Table A5 Source Code

- Traceability/compliance LLR
- Goodness
- Standards compliance
- Architecture compliance
- Integration complete

- Criteria
  - Satisfied by tool (partial/full)
  - Satisfied conventionally (partial/full)
  - What can go wrong
  - Assumptions
  - Additional activities



The great execution debate



Call for conviction

- Guilty of applying superior design approaches
- Use of circumstantial evidence vs. good forensics